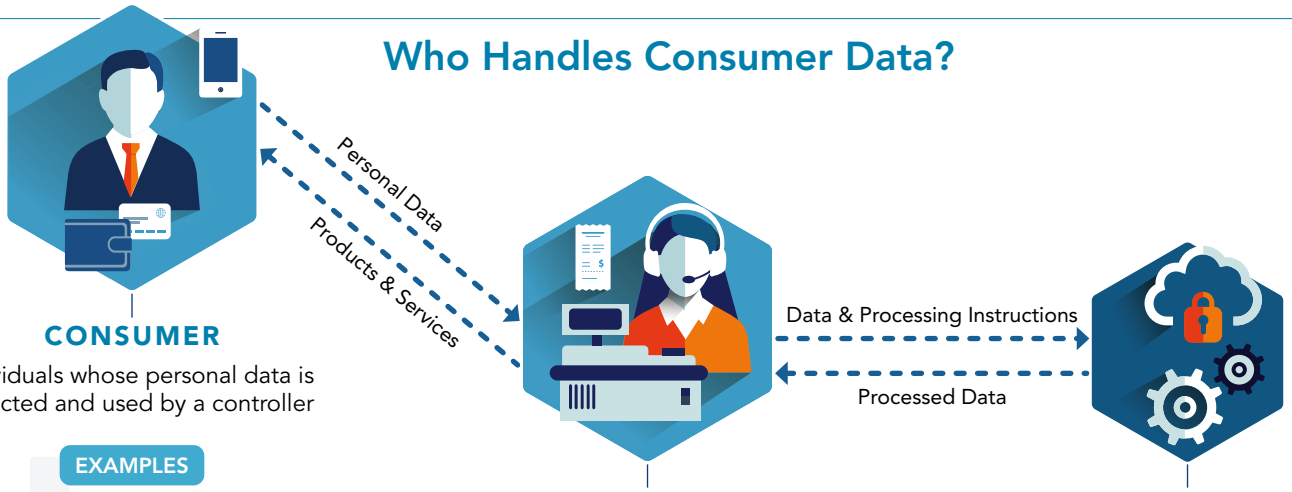
The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation

Comprehensive privacy legislation must create strong obligations for all companies that handle consumer data. These obligations will only be strong enough to protect consumer privacy and instill trust, though, if they reflect how a company interacts with consumer data.

Privacy laws worldwide distinguish between two types of companies: (1) businesses that decide *how* and *why* to collect consumer data, which act as **controllers** of that data and (2) businesses that process the data on *behalf of* another company, which act as **processors** of that data

This fundamental distinction is critical to a host of global privacy laws, including the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). Both types of businesses have important responsibilities and obligations, which should be set out in any legislation.

Who Handles Consumer Data?



CONSUMER

Individuals whose personal data is collected and used by a controller

EXAMPLES

Consumers who shop at retail stores, buy products online, or share information on social media platforms.

CONSUMERS SHOULD HAVE THE RIGHT TO:

- **Know** what type of data a controller collects — and why
- **Say no,** and opt out of broad types of use, not just sale
- **Access** information about them
- **Correct** that information
- **Delete** that information
- Have their data **securely protected**
- Have their data used **consistent with their expectations**

CONTROLLER

Decides whether and how to collect data from consumers, and the purposes for which that data is used

EXAMPLES

Companies that interact directly with consumers, such as hotels, banks, retail stores, travel agencies, and consumer-facing technology providers.

CONTROLLERS ARE RESPONSIBLE FOR:

Obtaining any consent needed to process a consumer's data

Responding to consumer requests for access, correction, or deletion

Using data consistent with the consumers' expectation

PROCESSOR

Processes data on behalf of a controller, pursuant to the controller's instructions

EXAMPLES

Companies that provide business-to-business products like cloud computing, and vendors like printers, couriers, and others that process data at the direction of another company.

PROCESSORS ARE RESPONSIBLE FOR:

Processing data consistent with a controller's instructions

Adopting appropriate safeguards designed to protect data security

Controllers and processors should have role-dependent responsibilities to ensure consumers' privacy and security are protected.

Privacy Laws Worldwide Distinguish Between Controllers and Processors

Privacy laws worldwide reflect the basic distinction between companies that decide to collect and use data about individuals and companies that only process such data.

Companies that decide how and why to collect consumer data.	Companies that process consumer data at the direction of others.
GDPR: Controllers Determine the "purposes and means" of processing.	**GDPR: Processors** Handle personal data "on behalf of" a controller.
CCPA: Businesses Determine the "purposes and means" of processing.	**CCPA: Service Providers** Handle personal information "on behalf of" businesses.

This distinction is crucial to a host of privacy laws beyond the GDPR and CCPA. In addition, leading international privacy standards, including ISO 27701, and voluntary frameworks that ensure data can be transferred across national borders, such as the APEC Cross Border Privacy Rules, also distinguish between controllers and processors.

EXAMPLE

A business contracts with a printing company to create invitations to an event. The business gives the printing company the names and addresses of the invitees from its contact database, which the printer uses to address the invitations and envelopes. The business then sends out the invitations.

The business is the controller of the personal data processed in connection with the invitations. The business decides the purposes for which the personal data is processed (to send individually-addressed invitations) and the means of the processing (mail merging the personal data using the invitees' addresses). The printing company is the processor handling the personal data pursuant to the business's instructions. The printing company cannot sell the data or use it for other purposes, such as marketing. If the printing company disregarded those limits and used the data for its own purposes, it would become a controller and be subject to all obligations imposed on a controller.

Why Is the Distinction Between Controllers and Processors Important to Protecting Consumer Privacy?

Distinguishing between controllers and processors ensures that privacy laws impose obligations that reflect a company's role in handling consumer data. This helps safeguard consumer privacy without inadvertently creating new privacy or security risks.

Data Security. Controllers and processors should both have strong obligations to safeguard consumer data.

- Placing this obligation on both types of companies ensures consumer data is protected.
- Controllers and processors should both employ reasonable and appropriate security measures, relative to the volume and sensitivity of the data, size, and nature of the business, and the cost of available tools.

Consumer Rights Requests. Responding to important consumer rights requests—such as requests to access, correct, or delete personal data—requires knowing what is in that data.

- Controllers interact with consumers and decide when and why to collect their data. For that reason, laws like the GDPR and CCPA require controllers to respond to consumer rights requests. Moreover, controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold.
- Processors, in contrast, often do not know the content of the data they process, and may be contractually prohibited from looking at it. It is not appropriate for processors to respond directly to a consumer's request—which creates both security risks (by providing data to consumers they do not know) and privacy risks (by looking at data they otherwise would not). Processors should instead provide controllers with tools the controller can use to collect data needed to respond to a consumer's request.